

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

At a session of the Public Service
Commission held in the City of
Albany on June 14, 2018

COMMISSIONERS PRESENT:

John B. Rhodes, Chair
Gregg C. Sayre
Diane X. Burman
James S. Alesi

CASE 18-M-0376 - Proceeding on Motion of the Commission
Regarding Cyber Security Protocols and
Protections in the Energy Market Place.

ORDER INSTITUTING PROCEEDING

(Issued and Effective June 14, 2018)

BY THE COMMISSION:

INTRODUCTION

For several months the Joint Utilities,¹ the Department of Public Service Staff, and numerous entities participating in the Energy Service Companies (ESCOs) marketplace have been dedicating significant attention to strengthening cyber security protections. While cyber protections have long been a priority

¹ The Joint Utilities consist of Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation (together the "Joint Utilities").

for the Commission and the industries it regulates,² a recent cyber event impacting the energy services market makes clear that additional attention is needed to ensure that appropriate protections are being implemented and followed throughout the industry. Cyber security threats have become a common occurrence, and the industry must be vigilant in order to protect against, detect, and respond to these events.

In the discussions that are being held among the Joint Utilities, Department Staff, and energy services entities,³ all parties agreed with the need for appropriate cyber security protections. The Joint Utilities are currently pursuing these business-to-business discussions pursuant to the Uniform Business Practices approved by the Commission in Case 98-M-1343.⁴ In those discussions, the Joint Utilities have requested that all energy services entities complete a Self-Attestation of Information Security Controls by the end of June 2018. Additionally, the Joint Utilities are requesting that energy services entities review and comment on proposed Data Security Agreements (DSAs) by June 22, 2018, and to be prepared to sign a final DSA by the end of July 2018. The attestations are designed to expeditiously identify any material gaps in current best practice cyber security controls. Any material gaps will need to be promptly remedied. Additional protections, including liability assurance, indemnification, audits, and cyber

² See, Case 16-M-0015, Petition of Municipal Electric and Gas Alliance, Inc. to Create a Community Choice Aggregation Pilot Program, Order Approving Community Choice Aggregation Program and Utility Data Security Agreement with Modifications (issued October 19, 2017) (CCA DSA Order).

³ Energy services entities includes ESCOs, Electronic Data Interchange (EDI) providers, and any other third party that contracts with an ESCO to communicate data between the ESCO and the utility.

⁴ Case 98-M-1343, In the Matter of Retail Access Business Rules.

insurance, are being addressed in the DSAs. Joint Utilities' proposed DSA is modeled after the DSA approved by the Commission in the CCA DSA Order. The Commission supports the business-to-business process described above, including the current deadlines, which have been agreed to by all parties.

It is essential to ensure that cyber security protections are being adequately addressed to mitigate vulnerability of utility systems to cyber-attacks, and to ensure that confidential and sensitive customer information remains safeguarded from potential data breaches. To support these goals, the Commission directs Department Staff to review the issues being addressed in the current business-to-business process between the Joint Utilities and energy service entities, and ensure that any issues that cannot be properly resolved in that forum are addressed in this proceeding. Department Staff is directed to, by August 31, 2018, file a report on the status of the business-to-business process undertaken to address cyber security issues. The Commission's goals are to ensure that adequate cyber security protections are in place to protect utility systems and confidential and sensitive customer information, and to explore whether insurance is an efficient and effective vehicle for mitigating any potential financial risks. These issues should be developed to address both the energy services entities, as well as distributed energy resource suppliers.

The Commission orders:

1. A proceeding is commenced to address cyber security protection described in the body of this Order.

2. In the Secretary's sole discretion, the deadlines set forth in this order may be extended. Any request for an extension must be in writing, must include a justification for

the extension, and must be filed at least one day prior to the affected deadline.

3. This proceeding is continued.

By the Commission,

(SIGNED)

KATHLEEN H. BURGESS
Secretary